REMARKS/ARGUMENTS

Reconsideration of this application is respectfully requested.

Rejection of claims 1-6 under 35 U.S.C. § 102 as allegedly anticipated by the newly cited Chang '425 reference is respectfully traversed.

In a nutshell, one major and fundamental distinction between applicants' claimed invention and any possible teaching or suggestion of Chang is: applicants' claims 1-6 require a server computer to validate a digital signature associated with the file requested by some other (e.g. client) computer—and the applicants claimed server computer/method denying access to the requested file by the requesting other computer if the digital signature is found to be invalid. That is, as has been previously explained, applicants claimed invention does not permit the requested file to be transmitted in any form to the requesting computer unless the digital signature is verified as valid. By thus denying any access to the requested file (i.e. it is never transmitted in any form to the requesting computer), applicants have addressed several possible adverse hacker schemes as described in the specification.

Chang is an example of the "second approach" (page 3 line 8 to page 6 line 10 of applicants' specification) in the prior art to the problem of authenticating digital files supplied to a user's computer. Although Chang is concerned with transmission of executable files whereas applicants exemplary embodiment concentrates on transmission of 'content' – e.g. web-pages this distinction is not important because applicants claims are not limited to authentication of content rather than executable code.

The concept of 'server' and 'client' computers connected via a computer network such as the Internet is, of course quite old. The World-Wide-Web involves server computers contactable at the WWW address www.uspto.go/serving web pages to client computers all over the world.

To give an example of the problem addressed by the present invention, suppose that the server computer at www.uspto.gov was compromised by anti-patent campaigners who then altered the web pages provided at that web address so that they had "Information Wants to be Free" stamped across them.

As noted, Chang's literal teaching is applied to executable computer code, but supposing, arguendo, that it were obvious to extend the idea to content, the Chang system still would not guarantee that users of client computers around the world would not see the altered web-page. This is because the users of the client computers might switch off a protection feature, or figure out how to read the altered web-page which even if 'deleted' would probably still be stored on the computer's hard-disk.

More particularly, Chang only teaches or suggests that authentication of the code should be done always at the client computer—lines 14-16 of the abstract discuss transmission to the client computer. It is therefore clear that authentication of the code takes place after transmission – i.e. at the client computer. The same order of events is seen in the 'Summary of Invention' section of col. 3 and everywhere else in Chang.

A problem with the Chang approach is that even though the code is "discarded" or "rejected" it is likely still stored somewhere on the user's computer and hence could be executed by a sufficiently knowledgeable user or perhaps its execution could be triggered by malicious code placed on the user's computer without his/her knowledge.

The applicants' approach is to guarantee that these problems cannot arise by not sending the code/content to the client computer in the first place (should the digital signature be found invalid).

Claim 1 is directed to steps carried out by a server computer. The only mentions of the 'other computer' – i.e. a client computer—are that a signal is received from the other computer (4th feature of claim 1) and that the other computer is denied access to the file if the file's digital signature is not validated (final feature of claim 1). In other words, the digital signature validation is carried out on the server computer according to the applicants' claimed invention.

In marked contrast, Chang carries out the digital signature creation steps on a server computer (the pre-transmission steps seen in col. 3 lines 15 to 34), but then the digital signature validation step is carried out on a client computer (the post-transmission steps seen in col. 3 lines 38 to 65). In between those two steps the file is always transmitted from the server computer to the client computer.

It is transmission of the file before validation that leads to the very problem addressed by the applicants' claimed invention.

Independent claim 4 is directed to a server computer which, inter alia, denies the "other" computer access to a requested computer file if the digital signature associated with that file is found to be invalid (by a validation process that occurs at the server computer).

Independent claim 5 is directed to a method of operating a server computer and it also requires the server computer to provide the "other" requesting computer with access to the requested computer file only if the digital signature associated therewith is found to be valid.

For reasons already noted, Chang is materially deficient with respect to at least these features of each independent claim. Accordingly, it is not believed necessary at this time to detail the further deficiencies of Chang with respect to these independent claims or the dependent claims.

The Examiner's attention is also directed to new claims 7-10. It will be seen that new independent claim 7 is directed to a method of operating a computer system comprising at least one server computer, client computers and a network interconnecting them, etc. This claim also requires the server computer to send a requested file to the requesting client computer <u>only</u> if its associated digital signature () is(are) found to be valid.

Independent claim 9 is directed to a method for operating a serving computer and it also requires, inter alia, sending the requested file to the other requesting computer only if the associated digital signature is found to be valid. Dependent claims 8 and 10 add yet further patentable distinction by requiring the digital signature to have been created by the server computer from the file using a signing key.

Accordingly, this entire application is now believed to be in allowable condition and a formal notice to that effect is respectfully solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: Larry S. Nixon
Larry S. Nixon
Reg. No. 25,640

LSN:dm
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100